CLAIM AMENDMENTS

Claims 20-33 and 70-94 are pending; claims 1-19 and 34-69 have been canceled herein; claims 28-33 are currently amended herein; and claims 70-94 are newly added herein.

Claims 1-19 (canceled)

20. (previously presented) A digital content encryption and decryption apparatus of a digital content transmission system comprising:

a protocol format generator located at a server location, said protocol format generator generating a copyright protection protocol in response to identity characters of a user transmitted to said server location from a terminal unit, said copyright protection protocol including a header and digital contents, said digital contents being encrypted, said header having information for decrypting and explaining the digital contents; and

a protocol format decoder located at said terminal unit, said protocol format decoder having a decryption algorithm, said protocol format decoder decrypting and replaying the digital contents according to the information of the header received from the protocol format generator.

21. (previously presented) The apparatus of claim 20, wherein the protocol format generator generates a user key by adding key information to a key generation algorithm and calculates a hash value by adding the user key to a hash algorithm, said protocol format generator encrypting a temporary validation key by using the user key, said header including user authorization information

with the hash value and the encrypted temporary validation key, said key information being formed to correspond to said identity characters of the user.

22. (previously presented) The apparatus of claim 20, wherein the protocol format decoder generates a user key by adding key information to a key generation algorithm and decrypts a temporary validation key, transmitted within said copyright protection protocol, by using the user key, said protocol format decoder decrypting the encrypted digital contents with the temporary validation key, said key information being formed to correspond to said identity characters of the user.

23. (previously presented) A digital content encryption and decryption apparatus of a digital content transmission system comprising:

a protocol format generator located at a server location, said protocol format generator generating a copyright protection protocol by generating key information using random numbers, said key information corresponding to identity characters of a user transmitted to said server location from a terminal unit, said copyright protection protocol including a header and encrypted digital information added to the header;

said protocol format generator applying said key information to a key generating algorithm to generate a user key utilized to generate a temporary validation key, said temporary validation key being encrypted to generate user authorization information, said header including said user authorization information;

a protocol format decoder for copyright protection located at said terminal unit, said protocol format decoder receiving and storing said key information and receiving said copyright protection protocol; and

said protocol format decoder generating a second user key in response to the received key information, analyzes said user authorization information in response to said second user key to determine whether the terminal unit is authorized to receive said encrypted digital information, and when said terminal unit is authorized to receive said encrypted digital information, utilizing said second user key to decrypt said temporary validation key from said user authorization information, the decrypted temporary validation key being used to decrypt said encrypted digital information.

24. (previously presented) The apparatus of claim 23, wherein the protocol format decoder generates said second user key by adding the stored key information to a second key generation algorithm.

25. (previously presented) A copyright protection protocol for protecting copyright of digital contents, said protocol including a header and the digital contents, said digital contents being encrypted, said header including key data for decrypting the digital contents, said key data being randomly generated in response to identity characters of a user transmitted to a host server from a terminal unit, wherein said terminal unit receives said protocol from said host server and replays said digital contents by decrypting the encrypted digital contents in response to the key data.

26. (original) The protocol of claim 25, further comprising a field for indicating the size of the encrypted digital contents, and an additional information field.

27. (original) The protocol of claim 25, wherein the header comprises a copyright support field for indicating whether the digital contents are under copyright protection, an unencrypted header field, and an encrypted header field.

28. (currently amended) The protocol of claim 25, wherein the header comprises a copyright support field for indicating whether the digital contents are under copyright protection, an unencrypted header field, a field for indicating the size of the unencrypted header field, an encrypted header field, and a field for indicating the size of the encrypted header field.

29. (currently amended) The protocol of claim 27 or 28, wherein the unencrypted header field comprises a copyright library version field, a digital content conversion format field, a key generation algorithm field, a digital content encryption algorithm field, a field for indicating user authorization information at [[PC]] personal computer, and a field for indicating user authorization information at a replaying device.

30. (currently amended) The protocol of claim 29, wherein the field for indicating user authorization information at the [[PC]] personal computer and the field for indicating user authorization information at the replaying device comprise a field for indicating a hash value of

[[the]] a user key, and a field for indicating the size of the hash value generated by a hash algorithm, a field for indicating a resultant value of an encrypted temporary validation key, and a field for indicating the size of the resultant value of the encrypted temporary validation key, respectively.

31. (currently amended) The protocol of claim 27 or 28, wherein the unencrypted header field comprises a copyright library version field, a digital content conversion format field, a field for indicating the code of a digital content provider, a key generation algorithm field, a digital content encryption algorithm field, a field for indicating the number of users sharing [[PC]] a personal computer, a field for indicating the number of users sharing a replaying device, a field for indicating user authorization information at the [[PC]] personal computer, and a field for indicating user authorization information at the replaying device.

32. (currently amended) The protocol of claim 31, wherein the field for indicating user authorization information at the [[PC]] personal computer and the field for indicating user authorization information at the replaying device comprise a field for indicating a hash value of [[the]] a user key, and a field for indicating the size of the hash value generated by a hash algorithm, a field for indicating a resultant value of an encrypted temporary validation key, and a field for indicating the size of the resultant value of the encrypted temporary validation key, respectively.

33. (currently amended) The protocol format of claim 27 or 28, wherein the encrypted header field comprises a field for an encryption algorithm of the digital content, a field for indicating a basic

process unit of the digital content, a field for indicating the number of encrypted [[byte]] bytes, and a hash value field for a hash value for determining a state of the entire header.

Claims 34-69 (canceled)

70. (new) Apparatus for decrypting and encrypting a digital content, comprising:

a terminal unit having a decryption algorithm, said terminal unit transmitting identity characters of a user, receiving and storing a key information, receiving a protocol including encrypted digital content, and decrypting said protocol by using said decryption algorithm and said key information; and

a service server having an encryption algorithm, said service server generating said key information corresponding to said identity characters transmitted from said terminal unit, transmitting said key information in a header to said terminal unit, encrypting said digital content by using said key information and said encryption algorithm, and transmitting said protocol including said encrypted digital content along with said header to said terminal unit.

71. (new) The apparatus of claim 70, wherein said terminal unit further comprises:

a key generation algorithm responsive to said key information for generating a user key, the user key being used for generating and confirming user authorization information by decrypting a temporary validation key in the user authorization information of the header, said temporary validation key being used for decrypting said encrypted digital content.

72. (new) The apparatus of claim 71, wherein said terminal unit further comprises:

an interface for receiving said key information generated by said service server;

a user authority identifier obtaining the user key after reading the header of the protocol received from the service server and identifying whether said user is authorized to receive said digital content by analyzing the user authorization information with the user key;

a temporary validation key decryptor for decrypting said temporary validation key by using the user key provided by said user authorization identifier; and

a digital content decryptor for decrypting said encrypted digital content by using the temporary validation key decrypted by the temporary validation key decryptor.

73. (new) The apparatus of claim 70, wherein said service server further comprises

a key generation algorithm responsive to said key information for generating a user key, the user key being used for encrypting a temporary validation key generated in response to a user's request, the temporary validation key being used for encrypting said digital content, the user key and the encrypted temporary validation key being used to generate user authorization key information, the header being generated in response to the user authorization key information.

74. (new) The apparatus of claim 73, wherein said service server further comprises:

an interface for receiving said identity characters input from said terminal unit;

a key information generator for generating said key information in response to said identity

characters received by said interface;

a user key generator responding to said key information for generating said user key;

a temporary validation key generator for generating said temporary validation key in response to a user access signal that is input through the interface;

a user authorization information generator responding to said user key for encrypting said temporary validation key to generate user authorization information;

a header generator responding to said user key for generating a header, wherein said header includes said user authorization information; and

a protocol format generator for adding said encrypted digital content to said header to generate said protocol.

75. (new) The apparatus of claim 70, further comprised of a service sanction agent server connected to said service server for receiving from the service server a signal concerning digital content fee responding to the transmission of said digital content requested by said user, and accumulating said digital content fees responding to said signal into a registered user's ID.

76. (new) The apparatus of claim 70, wherein the terminal unit having a network access program is connected to a network, public switched telephone network, or a wireless network.

77. (new) The apparatus of claim 73, wherein said service server further comprises a database storing a set of identity characters used by said key information generator for comparison

with the user's identity characters in order to determine whether the user is a registered user.

78. (new) The apparatus of claim 70, wherein said protocol is copyright protection protocol.

79. (new) An apparatus for encrypting and decrypting a digital content, comprising:

a terminal unit having a decryption algorithm, said terminal unit transmitting identity characters of a user, receiving and storing a key information, receiving a protocol including encrypted digital content, and decrypting said protocol by using said decryption algorithm and said key information;

a service server having encryption algorithm, said service server transmitting said key information to said terminal unit, encrypting said digital content by using said key information and said encryption algorithm, and transmitting said protocol to said terminal unit; and

a host server responding to said identity characters transmitted to said service server for generating said key information, for transmitting said key information to said service server, and for storing a set of identity characters to be used for comparison to the user's identity characters.

80. (new) The apparatus of claim 79, wherein said terminal unit further comprises:

a key generation algorithm responsive to said key information for generating a user key, the user key being used for generating and confirming user authorization information by decrypting a temporary validation key in the user authorization information of the header, said temporary validation key being used for decrypting said encrypted digital content.

81. (new) The apparatus of claim 79, wherein said terminal unit further comprises:

an interface for receiving said key information generated by said service server;

a user authority identifier obtaining the user key after reading the header of the protocol received from the service server and identifying whether said user is authorized to receive said digital content by analyzing the user authorization information with the user key;

a temporary validation key decryptor for decrypting said temporary validation key by using the user key provided by said user authorization identifier; and

a digital content decryptor for decrypting said encrypted digital content by using the temporary validation key decrypted by the temporary validation key decryptor.

82. (new) The apparatus of claim 79, wherein said service server further comprises:

a key generation algorithm responsive to said key information for generating a user key, the user key being used for encrypting a temporary validation key generated in response to a user's request, the temporary validation key being used for encrypting said digital content, the user key and the encrypted temporary validation key being used to generate user authorization key information, the header being generated in response to the user authorization key information.

83. (new) The apparatus of claim 79, wherein said service server further comprises:

an interface for receiving said identity characters input from said terminal unit;

key information generator responding to said identity characters for generating said key

information;

a user key generator responding to said key information for generating said user key;

a temporary validation key generator responding to a user's access to said service server for generating said temporary validation key;

a user authorization information generator responding to said user key for encrypting said temporary validation key to generate user authorization information;

a header generator responding to said user key for generating the header, wherein said header includes said user authorization information; and

a protocol format generator for adding said encrypted digital content to said header to generate said protocol.

84. (new) The apparatus of claim 79, wherein said host server further comprises:

a key information generator corresponding to the identity characters input from said interface for generating said key information.

85. (new) The apparatus of claim 79, further comprising:

a service sanction agent server connected to said service server for receiving from the service server a signal concerning a digital content fee responding to said transmission of the digital content requested by said user, and accumulating the digital content fees, in response to said signal, into memory corresponding to a registered user's ID.

86. (new) The apparatus of claim 79, wherein said terminal unit is connected to a network, public switched telephone network, or wireless network, said terminal unit having a network access program to access said service server.

87. (new) The apparatus of claim 79, wherein said host server further comprises a database storing said set of identity characters used by said key information generator for comparison with the user's identity characters in order to determine whether the user is a registered user.

88. (new) The apparatus of claim 79, wherein said protocol is a copyright protection protocol.

89. (new) A method for encrypting digital content, comprising steps of:

inputting from a terminal unit identity characters of a user for registration;

determining whether said user is registered;

storing information of said identity characters of said user on membership registration when said user is determined to be unregistered;

transmitting key information to said user;

encrypting said digital content by using a temporary validation key in response to a request signal from said user; and

transmitting to said terminal unit a copyright protection protocol including said encrypted digital content and a header, said header including user authorization information and said temporary

validation key.

90. (new) The method of claim 89 further comprising a step of transmitting information relating to a service fee to a service sanction agent server, said information being generated when said encrypted digital content is transmitted to said terminal unit.

91. (new) A method for encrypting digital content, comprising steps of:

receiving from a terminal a request signal for digital content from a user;

generating a user authorization information when said request signal is received;

generating a header having information relating to said digital content and said user authorization information;

encrypting said digital content; and

transmitting a copyright protection protocol including said encrypted digital content and said header.

92. (new) The method of claim 9, wherein said authorization information is generated by using key information relating to said user's identity characters.

93. (new) The method of claim 91, wherein said step of generating said user authorization information further comprises steps of:

generating a temporary validation key in response to said received request signal;

generating a user key by using key information; and

generating said user authorization information by using said temporary validation key and said user key.

94. (new) The method of claim 93, wherein said user authorization information includes a hash value of said user indicating user's authorization.